UNCLASSIFIED

Mozilla FireFox

Version: 4

Release: 2

23 April 2010

STIG.DOD.MIL

Sort Order: Group ID (Vulid), ascending order
Notice: Developed by DISA for the DoD
Description:

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System= SECRET Checklist
Top Secret System = SECRET Checklist

Group ID (Vulid): V-6318
Group Title: DTBG010-DoD Root Certificate is not installed
Rule ID: SV-6388r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBG010
Rule Title: The DOD Root Certificate is not installed.

Vulnerability Discussion: The DOD root certificate will ensure that the trust chain is established for server certificate issued from the DOD CA.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedures: Open Internet Explorer. From the menu bar select Tools. From the Tools dropdown menu, select the Internet Options. From the Internet Options window, select the Content tab, from the Content tab window select the Publishers… button, from the Publisher window select the Trusted Root Certification Authorities Tab. Scroll through the Certificate Authorities list. Look for the DoD Class 3 Root CA. Click on DoD Class 3 Root CA. Select the View button. From the View Window select the Details Tab

Scroll to the bottom of the Window and select Thumbprint Algorithm in the bottom Pane you should see “sha1”, Next select Thumbprint

Criteria:
If there is no entry for the DoD Class 3 Root CA, then this is a Finding.

If the value of the Thumbprint Algorithm “sha1” and Thumbprint field is not: DoD Class 3 Root CA certificate is not:
10 f1 93 f3 40 ac 91 d6 de 5f 1e dc 00 62 47 c4 f2 5d 96 71,
then this is a Finding.

Check Content:
Procedure: Use the Tools/Options/Advanced/Encryption dialog. On the Select the View Certificates button. On the Certificate Manager window, select the Authorities tab. Scroll through the Certificate Name list to the U.S. Government heading. Look for the entry for the DoD Class 3 Root CA.
If there is an entry for the DoD Class 3 Root CA, select the entry and then the View button. On the Certificate Viewer window, determine the value of the MD5 Fingerprint field.

Criteria:
If there is no entry for the DoD Class 3 Root CA, then this is a Finding.

If the value of the MD5 Fingerprint field of the DoD Class 3 Root CA certificate is not:
8C:48:08:65:BB:DA:FF:9F:FD:8C:E2:95:E0:96:B9:9D,

then this is a Finding.

If the value of the SHA1 Fingerprint field of the DoD Class 3 Root CA certificate is not: 10:F1:93:F3:40:AC:91:D6:DE:5F:1E:DC:00:62:47:C4:F2:5D:96:71,then this is a Finding.

Fix Text: Install the DOD root certificate.

Group ID (Vulid): V-15767
Group Title: DTBF020 - FireFox Preferences–Use of SSL Version 3
Rule ID: SV-16706r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF020
Rule Title: Firefox is configured to allow use of SSL 3.0.

Vulnerability Discussion: DoD implementations of SSL must use TLS 1.0 in accordance with the Network Infrastructure STIG. Earlier versions of SSL have known security vulnerabilities and are not authorized for use in DOD. Firefox has this set to on by default but this is not apparent in the GUI options screen.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a browser window, type "about:config" in the address bar, then navigate to the setting for Preference Name "security.enable_ssl3: and set value to 'false" and locked.

Criteria: If the value of "security.enable_ssl3" is false, this is not a finding. If the value is locked, this is not a finding.

Fix Text: Set the preference "security.enable_ssl3" to "false" and lock using the Mozilla.cfg file.

Group ID (Vulid): V-15768
Group Title: DTBF050 - FireFox Preferences – Verification
Rule ID: SV-16707r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF050
Rule Title: FireFox is not configured to ask which certificate to present to a web site when a certificate is required.

Vulnerability Discussion: When a web site asks for a certificate for user authentication, Firefox must be configured to have the user choose which certificate to present. Websites within DOD require user authentication for access which increases security for DoD information. Access will be denied to the user if certificate management is not configured.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Type "about:config" in the browser address bar. Verify Preference Name "security.default_personal_cert" is set to "Ask Every Time" and is locked to prevent the user from altering.

Criteria: If the value of "security.default_personal_cert" is set incorrectly or is not locked, then this is a finding.

Fix Text: Set the value of "security.default_personal_cert" to "Ask Every Time". Use the Mozilla.cfg file to lock the preference so users cannot change it.

Group ID (Vulid): V-15770
Group Title: DTBF100 -FireFox Preferences–auto-download actions
Rule ID: SV-16709r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF100
Rule Title: Firefox automatically executes or downloads MIME types which are not authorized for auto-download.

Vulnerability Discussion: The default action for file types for which a plugin is installed is to automatically download and execute the file using the associated plugin. Firefox allows you to change the specified download action so that the file is opened with a selected external application or saved to disk instead. View the list of installed browser plugins and related MIME types by entering about:plugins in the address bar.

When you click a link to download a file, the MIME type determines what action Firefox will take. You may already have a plugin installed that will automatically handle the download, such as Windows Media Player or QuickTime. Other times, you may see a dialog asking whether you want to save the file or open it with a specific application. When you tell Firefox to open or save the file and also check the option to "Do this automatically for files like this from now on", an entry appears for that type of file in the Firefox Applications panel, shown below.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Use Method 1 or 2 to check if the following extensions are listed in the browser configuration: HTA, JSE, JS, MOCHA, SHS, VBE, VBS, SCT, WSC. By default, most of these extensions will not show up on the Firefox listing.

Criteria:

Method 1: In about:plugins, Installed plug-in, inspect the entries in the Suffixes column.

If any of the prohibited extensions are found, then for each of them, verify that it is not associated with an application that executes code. However, applications such as Notepad.exe that do not execute code may be associated with the extension. If the extension is associated with an unauthorized application, then this is a finding.

If the extension exists but is not associated with an application, then this is a finding.

Method 2:
Use the Options User Interface Applications menu to search for the prohibited extensions in the Content column of the table.

If an extension that is not approved for automatic execution exists and the entry in the Action column is associated with an application that does not execute the code (e.g., Notepad), then do not mark this as a finding.

If the entry exists and the "Action" is 'Save File' or 'Always Ask', then this is not a finding.

If an extension exists and the entry in the Action column is associated with an application that does/can execute the code, then this is a finding.

Fix Text: Remove any unauthorized extensions from the autodownload list.

Group ID (Vulid): V-15771
Group Title: DTBF105 - FireFox Preferences – Shell Protocol
Rule ID: SV-16710r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF105
Rule Title: Network shell protocol is enabled in FireFox.

Vulnerability Discussion: Although current version of Firefox have this set to disabled by default, use of this option can be harmful. This would allow the browser to access the Windows shell. This could allow access to the underlying system. This check verifies that the default setting has not been changed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Open a browser window, type "about:config" in the address bar.

Criteria: If the "network.protocol-handler.external.shell" value is "false", then this is not a finding.

Fix Text: Set the "network.protocol-handler.external.shell" value to "false"

Group ID (Vulid): V-15772
Group Title: DTBF110 - FireFox Preferences – Open Confirmation
Rule ID: SV-16711r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF110
Rule Title: Firefox not configured to prompt user before download and opening for required file types.

Vulnerability Discussion: New file types cannot be added directly to the helper applications or plugins listing. Files with these extensions will not be allowed to use Firefox publicly available plugins and extensions to open. The application will be configured to open these files using external applications only. After a helper application or save to disk download action has been set, that action will be taken automatically for those types of files. When the user receives a dialog box asking if you want to save the file or open it with a specified application, this indicates that a plugin does not exist. The user has not previously selected a download action or helper application to automatically use for that type of file. When prompted, if the user checks the option to Do this automatically for files like this from now on, then an entry will appear for that type of file in the plugins listing and this file type is automatically opened in the future. This can be a security issue. New file types cannot be added directly to the Application plugin listing.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a browser window, type "about:config" in the address bar.

Criteria: If the “plugin.disable_full_page_plugin_for_types” value is not set to include the following external extensions and not locked, then this is a finding:

PDF, FDF, XFDF, LSL, LSO, LSS, IQY, RQY, XLK, XLS, XLT, POT PPS, PPT, DOS, DOT, WKS, BAT, PS, EPS, WCH, WCM, WB1, WB3, RTF.

Fix Text: Ensure the following extensions are not automatically opened by Firefox without user confirmation. Do not use plugins and add-ons to open these files. Use the "plugin.disable_full_page_plugin_for_types" preference to set and lock the following extensions so that an external application rather than an add-on or plugin will not be used. (PDF, FDF, XFDF, LSL, LSO, LSS, IQY, RQY, XLK, XLS, XLT, POT PPS, PPT, DOS, DOT, WKS, BAT, PS, EPS, WCH, WCM, WB1, WB3, RTF)

Group ID (Vulid): V-15773
Group Title: DTBF120 - FireFox Preferences – ActiveX controls
Rule ID: SV-16712r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF120
Rule Title: FireFox plug-in for ActiveX controls is installed.

Vulnerability Discussion: When an ActiveX control is referenced in an HTML document, MS Windows checks to see if
the control already resides on the client machine. If not, the control can be downloaded from a
remote web site. This provides an automated delivery method for mobile code.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a browser window, type "about:plugins" in the address bar.

Criteria: If the Mozilla ActiveX control and plugin support is present and enabled, then this is a finding.

Fix Text: Remove/uninstall the Mozilla ActiveX plugin

Group ID (Vulid): V-15774
Group Title: DTBF140 - FireFox Preferences – Autofill forms
Rule ID: SV-16713r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF140
Rule Title: Firefox formfill assistance option is disabled.

Vulnerability Discussion: In order to protect privacy and sensitive data, Firefox provides the ability to configure Firefox such that data entered into forms is not saved. This mitigates the risk of a website gleaning private information from prefilled information.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Type "about:config" in the address bar, verify that the preference name “browser.formfill.enable" is set to “false” and locked.

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference “browser.formfill.enable" is set and locked to the value of “False”.

Group ID (Vulid): V-15775
Group Title: DTBF150 - FireFox Preferences – Autofill passwords
Rule ID: SV-16714r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF150
Rule Title: Firefox is configured to autofill passwords.

Vulnerability Discussion: While on the internet, it may be possible for an attacker to view the saved password files and gain access to the user's accounts on various hosts.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
In About:Config, verify that the preference name “signon.prefillForms“ is set to “false” and locked.

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference " signon.prefillForms " is set and locked to the value of “False”.

Group ID (Vulid): V-15776
Group Title: DTBF160 - FireFox Preferences – Password store
Rule ID: SV-16715r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF160
Rule Title: FireFox is configured to use a password store with or without a master password.

Vulnerability Discussion: Firefox can be set to store passwords for sites visited by the user. These individual passwords are stored in a file and can be protected by a master password. Autofill of the password can then be enabled when the site is visited. This feature could also be used to autofill the certificate pin which could lead to compromise of DoD information.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Type "About:Config" in the browser window. Verify that the preference name “signon.rememberSignons" is set and locked to “false”.

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference "“signon.rememberSignons“ is set and locked to the value of “false”.

Group ID (Vulid): V-15777
Group Title: DTBF170 - FireFox Preferences – Cookies
Rule ID: SV-16716r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF170
Rule Title: Firefox does not clear cookies upon closing.

Vulnerability Discussion: Cookies can help websites perform better but can also be part of spyware. To mitigate this risk, set browser preferences to perform a Clear Private Data operation when closing the browser in order to clear cookies and other data installed by websites visited during the session.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Type "about:config" in the address bar of the browser. Verify that the preference “privacy.sanitize.sanitizeOnShutdown" is set to “true”. Also “privacy.sanitize.promptOnSanitize” must be set to “false” to prevent users from circumventing the deleting of cookies. Both settings must also be locked to prevent user changes.

Criteria: If the parameter for either of the two sanitize preferences is set incorrectly, then this is a finding. If the settings are not locked, then this is a finding.

Fix Text: Ensure the preference "privacy.sanitize.sanitizeOnShutdown" is set and locked to the value of “true”. Also ensure the preference “privacy.sanitize.promptOnSanitize” is set and locked to “false”

Group ID (Vulid): V-15778
Group Title: DTBF180 - Pop-up windows
Rule ID: SV-16717r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF180
Rule Title: FireFox is not configured to block pop-up windows.

Vulnerability Discussion: Popup windows may be used to launch an attack within a new browser window with altered settings. This setting blocks popup windows created while the page is loading.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
In About:Config, verify that the preference name “dom.disable_window_open_feature.status " is set to “true” and locked.

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference "dom.disable_window_open_feature.status " is set and locked to the value of “true”.

Group ID (Vulid): V-15779
Group Title: DTBF181 - JavaScript move or resize windows
Rule ID: SV-16718r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF181
Rule Title: FireFox is configured to allow JavaScript to move or resize windows.

Vulnerability Discussion: JavaScript can make changes to the browser’s appearance. This activity can help disguise an attack taking place in a minimized background window. Set browser setting to prevent scripts on visited websites from moving and resizing browser windows.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
In About:Config, verify that the preference name “dom.disable_window_move_resize" is set and locked to “true”.

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference "dom.disable_window_move_resize" is set and locked to the value of “true”.

Group ID (Vulid): V-15982
Group Title: DTBF010 - Firefox Preferences - SSL 2.0 Protocol
Rule ID: SV-16924r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF010
Rule Title: The Firefox SSLV2 parameter is configured to allow use of SSL 2.0.

Vulnerability Discussion: Use of versions prior to TLS 1.0 are not permitted because these versions are non-standard. SSL 2.0 and SSL 3.0 contain a number of security flaws. These versions must be disabled in compliance with the Network Infrastructure and Secure Remote Computing STIGs. SSL 2.0 setting does not appear in the Options dialog and must be disabled using About:Config.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a browser window, type "about:config" in the address bar, then navigate to the setting for Preference Name "security.enable_ssl2" and verify the value is set to "false".

Criteria: If the parameter is set incorrectly, then this is a finding. If the value is not locked this is a finding.

Fix Text: Ensure the preference "security.enable_ssl2" is set to "false".

Group ID (Vulid): V-15983
Group Title: DTBF030 - Firefox Preferences – SSL Protocols TLS
Rule ID: SV-16925r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF030
Rule Title: Firefox is not configured to allow use of TLS 1.0.

Vulnerability Discussion: DoD implementations of SSL must use TLS 1.0 in accordance with the Network Infrastructure STIG. Earlier versions of SSL have known security vulnerabilities and are not authorized for use in DOD.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Open a browser window, type "about:config" in the address bar. Verify Preference Name "security.enable_tls" is set to the value "true" and locked.

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference value of "security.enable_tls" is set to "true" and locked.

Group ID (Vulid): V-15985
Group Title: DTBF182 - JavaScript raise or lower windows
Rule ID: SV-16927r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF182
Rule Title: Firefox is configured to allow JavaScript to raise or lower windows.

Vulnerability Discussion: JavaScript can make changes to the browser's appearance. Allowing a website to use JavaScript to raise and lower browser windows may disguise an attack. Browser windows may not be set as active via JavaScript.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
In About:Config, verify that the preference name "dom.disable_window_flip" is set and locked to "true".

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference "dom.disable_window_flip" is set and locked to the value of "true".

Group ID (Vulid): V-15986
Group Title: DTBF183 - JavaScript Context Menus
Rule ID: SV-16928r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF183
Rule Title: Firefox is configured to allow JavaScript to disable or replace context menus.

Vulnerability Discussion: A context menu (also known as a pop-up menu) is often used in a graphical user interface (GUI) and appears upon user interaction (e.g., a right mouse click). A context menu offers a limited set of choices that are available in the current state, or context, of the operating system or application. A website may execute JavaScript that can make changes to these context menus. This can help disguise an attack. Set this preference to "false" so that webpages will not be able to affect the context menu event.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Type "about:config" in the address bar of the browser. Verify that the preference "dom.event.contextmenu.enabled" is set and locked to "false".

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference "dom.event.contextmenu.enabled" is set and locked to the value of "false".

Group ID (Vulid): V-15987

Group Title: DTBF184 - JavaScript hiding or changing status bar
Rule ID: SV-16929r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF184
Rule Title: Firefox is configured to allow JavaScript to hide or change the status bar.

Vulnerability Discussion: When a user visits some webpages, JavaScript can hide or make changes to the browser's appearance to hide unauthorized activity. This activity can help disguise an attack taking place in a minimized background window. Determines whether the text in the browser status bar may be set by JavaScript. Set and lock to True (default in Firefox) so that JavaScript access to preference settings for is disabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Type "about:config" in the address bar of the browser. Verify that the preference "dom.disable_window_status_change" is set and locked to "true".

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference "dom.disable_window_status_change" is set and locked to the value of "true".

Group ID (Vulid): V-15988
Group Title: DTBF185 -JavaScript can change the status bar text
Rule ID: SV-16930r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF185
Rule Title: Firefox is configured to allow JavaScript to change the status bar text.

Vulnerability Discussion: JavaScript can make changes to the browser's appearance. This activity can help disguise an attack taking place in a minimized background window. Webpage authors can disable many features of a popup window that they open. Setting these preferences to true will override the author's settings and ensure that the feature is enabled and present in any popup window. This setting prevents the status bar from being hidden.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
In About:Config, verify that the preference "dom.disable_window_open_feature.status" is set and locked to "true".

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference "dom.disable_window_open_feature.status" is set and locked to the value of "true".

Group ID (Vulid): V-15989
Group Title: Sun AnswerBook2 HTTP GET Overflow
Rule ID: SV-16931r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBF130
Rule Title: Firefox is not configured to provide warnings when a user switches from a secure (SSL-enabled) to a non-secure page.

Vulnerability Discussion: Users may not be aware that the information being viewed under secure conditions in a previous page are not currently being viewed under the same security settings.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Type "about:config" in the browser window. Verify that the preference name “security.warn_leaving_secure" is set to “true” and locked.

Criteria: If the parameter is set incorrectly, then this is a finding. If the setting is not locked, then this is a finding.

Fix Text: Ensure the preference “security.warn_leaving_secure" is set to “true” and locked on this setting.

Group ID (Vulid): V-17988
Group Title: Fedora update for mediawiki - March 2008
Rule ID: SV-19509r2_rule
Severity: CAT I
Rule Version (STIG-ID): DTBF003
Rule Title: Installed version of Firefox unsupported.

Vulnerability Discussion: Use of versions of an application which are not supported by the vendor are not permitted. Vendors respond to security flaws with updates and patches. These updates are not available for unsupported version which can leave the application vulnerable to attack.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Method 1: View the following registry key:
HKLM\Software\Mozilla\Mozilla Firefox\CurrentVersion

Method 2: Search for the firefox.exe file using the search feature of the operating system. Examine the files properties for the product version (not the file version. For Windows OS, determine the version of the file by examining navigating to Properties/Version/Product Version. Examine for all instances of firefox.exe that are present on the endpoint.

Criteria: If the version number of the firefox.exe file is less than 3.x.x, then this is a Finding.

Fix Text: Upgrade the version of the browser to an approved version by obtaining software from the vendor or other trusted source.

UNCLASSIFIED